National Infrastructure Protection Center
CyberNotes

Issue #15-99 *July 21, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between July 3 and July 16, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold.**

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix[1]	Klock	User with physical access can bypass the screen save, gaining access to the current session	No vendor supplied patch or workaround available at time of publishing.	Klock bypass	Low	Bug discussed in newsgroups and websites.
Netscape[2]	Communicator v 4.6 (Linux) Communicator V 4.51 and 4.61 (Windows)	Even with "originating server" restrictions enabled on the browser, cookies may be accepted from third party site when JavaScripting is enabled.	Workaround: Disable JavaScripting.	Netscape cookie acceptance problem	Low	Bug discussed in newsgroups and websites.

[1] Securiteam Advisory, July 7, 1999.
[2] Bugtraq, July 9, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Hewlett-Packard[3]	CDE	When the PATH variable is constructed from several sources with the result that PATH contains the string "::", this is interpreted as the current directory. This can result in increased privileges.	The Vendor in a security bulletin has supplied workaround.	CDE path directory problem	Medium	Bug discussed in newsgroups and websites.
Microsoft[4]	Internet Information Server (IIS) running on NT Servers	Due to the server's inability to distinguish between pages that use SSL and those that do not, an unauthorized user can create a Denial-of-Service condition.	No vendor supplied patch or workaround available at time of publishing. Newsgroup suggested workaround is to separate secure and non-secure content onto different servers.	NT ISS SSL Denial-of-Service	Low	Bug discussed in newsgroups and websites.
ThirdVoice[5]	ThirdVoice	It is possible for an unauthorized user to insert code into the Third Voice application, which has the potential to capture user information. This captured information will be supplied to the original site the user was attempting to access and e-mailed to a hacker's e-mail account.	No vendor supplied patch or workaround available at time of publishing. Earlier posted fix corrects a similar problem but does not correct this problem	ThirdVoice ISAPI command problem	Medium/ High	Bug discussed in newsgroups and websites. Exploit has been published.
Unix[6] - Multiple systems	PINE	It is possible for an unauthorized individual to cause the remote system to execute a program or script. This occurs when the attacker sends an e-mail that contains uuencoded/uudecode characters and an attached index.html file.	Patches are available from most vendors for this problem	PINE uuencode/ uudecode code execution	Medium/ High	Bug discussed in newsgroups and websites. Exploit has been published.
University College London[7]	Session Directory (SDR)	An attacker can execute code with the privileges of the SDR user. This is accomplished by embedding TCL commands inside the packets used for incoming announcements.	Vendor recommends upgrading to version 2.6.3	SDR vulnerable	Medium/ High	Bug discussed in newsgroups and websites. Exploit has been published.

[3] HPSBUX9907-100, July 8, 1999.
[4] Bugtraq, July 7, 1999.
[5] Wired News, "Third Voice Patches Holes", July 12, 1999.
[6] Securiteam Advisory, "HHP-Pine remote exploit", July 7, 1999.
[7] Securiteam Advisory, "SDR vulnerable to attack", July 10, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Netscape[8]	Enterprise Server using SSL	An attacker can cause the Enterprise server to crash by starting a SSL 2.0 format session and sending more bytes then specified in the header.	Vendor supplied patch can be found at: http://help.netscape.com/business/filelib.html#SSLHandshake	Enterprise Server SLL handshake problem	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Axent[9]	ESM 5.0	Under specific conditions ESM will copy the user's startup script to the /TMP directory which changes file ownership and permissions to "root." When these files are copied back to the user's directory, the file ownership and permissions remain as root. This prevents the user from executing the startup script.	Vendor recommended solution is to use version 5.01 when available.	Axent User Profile permission vulnerability	Low/ Medium	Bug discussed in newsgroups and websites. The application causes this denial-of-service condition.
BMC software[10]	Patrol v3.2 (most Unix platforms)	The out of the box configuration may allow a local user to compromise root. This occurs when snmpagnt creates a file. The file is owned by the owner of the parent directory and is potentially world writeable. The local user can specify any file to create including '.rhost'.	No vendor supplied patch or workaround available at time of publishing.	Patrol SNMP agent file creation/ permission vulnerability	**High**	Bug discussed in newsgroups and websites. The application out of the box causes this problem.
Linux[11]	Linux kernel 2.0.37	If a non-standard memory configuration has been chosen, it is possible for a non-privilege user to gain root access.	This vulnerability is specific to kernel 2.0.37 with a non-standard memory configuration. Vendors recommend using later kernels if a non-standard memory configuration is required.	Linux segment limit vulnerability	**High**	Bug discussed in newsgroups and websites. The application out of the box causes this problem.
IBM[12]	AIX v4.2 through v4.3.1	It is possible for a malicious local user to cause a Denial-of-Service attack using the adb debugger shipped with the AIX operating system.	Vendor fix available at: ftp://aix.software.ibm.com/aix/efixes/security/adb_hang.tar.Z	AIX adb vulnerability	Low	Bug discussed in newsgroups and websites. Demonstration code has been made available.

[8] Bugtraq, July 6, 1999.
[9] Bugtraq, July 13, 1999.
[10] Bugtraq, July 13, 1999.
[11] Bugtraq, July 13, 1999.
[12] Bugtraq, July 12, 1999.

Hardware/ Operating System/ Vendor	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Unix[13] - Various	Systems based on BSD 4.4 code	It is possible to bypass rlimits using "mmap" and "shmget." If pagefaults are triggered, the system will quickly run out of memory result in a Denial-of-Service condition.	No vendor supplied patch or workaround available at time of publishing.	Shared memory denial-of-service	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Sun[14]	Java Hotspot with Microsoft Internet Information Server (IIS)	A specific URL will cause a system crash when IIS and Java HotSpot Performance engine are running together.	No vendor supplied patch or workaround available at time of publishing.	Java HotSpot Denial-of-Service vulnerability	Low	Bug discussed in newsgroups and websites. Exploit has been published.
Apple[15]	MacOS	Passwords for MacOS are easily cracked.	No vendor supplied patch or workaround available at time of publishing.	MacOS weak password encryption	Medium/ High	Bug discussed in newsgroups and websites. Exploit has been published.
Sun Solaris[16] - Multiple versions	Rpc.cmsd (Operating System)	Remote unauthorized user can execute a buffer overflow in the calendar manager that may result in root access.	No vendor supplied patch or workaround available at time of publishing.	Solaris rpc.cmsd Buffer Overflow	**High**	Bug discussed in newsgroups and websites. Exploit has been published.
WebTrends[17]	WebTrends for Firewalls v1.2 WebTrends Security Analyzer v2.0 WebTrends Log Analyzer v4.51 WebTrends Professional Suite v3.01	WebTrends running on NT using MAPI store NT service account and password information in a file with "Everyone: Full Access." The service account is an Administrator account and can lead to full system compromise.	Recommendation is to remove the "Everyone: Full Access" and add "Administrators: Full Control."	Bad Permissions on stored passwords by WebTrends	**High**	Bug discussed in newsgroups and websites.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, and root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

[13] Bugtraq, July 15, 1999.
[14] NTBugtraq, July 6, 1999.
[15] Bugtraq, July 9, 1999.
[16] Bugtraq, July 9, 1999.
[17] ISS Security Advisory, reissued July 3, 1999.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a "High" threat.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between July 3 and July 16, 1999, listed by date of script, script name, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 13 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script (Reverse Chronological Order)	**Script Name**	**Script Description**	**Comments**
July 15, 1999	**MacOS Pass 2.1**	**Password cracking program for MacOS.**	
July 15, 1999	Vm-dos.c	Program that exploits the shared memory vulnerability in Unix systems based on BSD 4.4 code.	
July 13, 1999	**Flushot.c**	**Exploit that drops network connections on windows 95/98.**	**This should not be confused with the anti-virus program with a similar name**
July 13, 1999	Segment-bug.c	Program that exploits the segment vulnerability in Linux kernel 2.0.37.	
July 12, 1999	Infect.c	Program that creates e-mail used to exploit the HHP-PINE remote exploit. See "Bugs, Holes & Patches - HHP PINE remote exploit" July 21, 1999.	
July 10, 1999	**MacPass**	**Password cracker for MacOS.**	
July 9, 1999	Cmsd-exploit.c	Program that exploit the buffer overflow in Sun to gain remote root access.	
July 8, 1999	Brutus	A password cracker.	
July 7, 1999	Pagoo	This is a Perl script that attempts all possible 4-digit passwords for the Pagoo Internet voice Mailbox.	
July 6, 1999	Mayar13.c	Program that sends illegal ICMP-timestamp packets to Windows 95/98 machines. This results in a Denial-of-Service attack.	
July 6, 1999	Nesexploit.c	Program that utilizes the SSL handshake problem in Netscape Enterprise Server to create a Denial-of-Service condition.	
July 5, 1999	Pandora v4.0	Vulnerability assessment tool that runs on Microsoft Windows or Linux. This tool is described as the SATAN for Netware.	
July 2, 1999	**Kod.c v1.2**	**Malformed IGMP header exploit which will bluescreen windows and kill TCP stack. Exploit works on BSD/Linux/*nix/Windows 98/2000.**	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

NESSUS

Nessus is a multi-purpose scanner, vulnerability/exploit analyzer that has been used by hackers/crackers as an attack tool. Root is required to run the server portion of the program. The Nessus server is implemented as a UNIX daemon and can be initiated automatically upon startup. There are numerous command line options that provide diagnostic information. This tool has a modular architecture, which allows individual programmers the flexibility to add modules that will check for specific vulnerabilities.

The stated philosophy behind this program is to provide a tool that is very easy to use. The program has reached that goal. The tool provides an intuitive GUI interface that is easy to use and demonstrates sophisticated programming skills. Complete instructions are provided as well.

Trends

Trends for this two week period:

1. Well-known security holes for which patches were previously available are being used by crackers to break into web sites.
2. Security holes in CGI scripts are currently being exploited.
3. An increased number of reports of SYN and IP Spoofing attacks that result in a Denial-of-Service.
4. Large numbers of Sun systems are being attacked using the calendar manager (rpc.cmsd).
5. Web hacks using Cold fusion vulnerabilities continues.
6. A number of attacks against IRIX and Solaris machine using the autofsd vulnerability have occurred recently.
7. Backdoors have been discovered that put root shells on IRIX systems (port courier 530) and Solaris systems (ingreslock 1524).
8. Hackers have taken a greater interest in cable modems and DSL lines. Individuals report receiving two probes per day against their machines using cable modems or DSL lines.

Viruses/Trojans

Hack 'a' Tack v1.20 - This Trojan horse is mainly a file transfer server. Due to its relatively small size, it has been used to transfer more powerful Trojan horses to the victim's machine. Many of the most popular anti-virus programs do not detect this Trojan horse. One method that has been recommended on mailing lists to remove this Trojan horse is to check for HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\ with Explorer32="C:\windows\Exp132.exe and remove this entry then go to the windows directory and remove Exp132.exe.

SSHD Trojan - This Trojan has a few changes to the normal SSH including a backdoor password (sexygurl) which provides access at as any user and connections to a user selected port will not be log by SSH. The default port that is not logged is 31337. This Trojan has recently been install by unauthorized individuals during system break-ins.

ICQMAPI.DLL false positive - Symantec has confirmed that Norton Anti-virus incorrectly identifies the file ICQMAPI.DLL has containing a Trojan horse. Symantec released a new updated definition that corrects this misidentification.

WinSATAN Trojan - This Trojan horse starts an FTP daemon on port 999. The default directory for the FTP server is C:/TEMP with no username/password. This Trojan connects to an IRC server sending a message "Online! I am ….., I use ….., my CPU is a ….." It also gives the attacker the ability to format the victim's hard-drive.